F1

Requested Patent: JP2003015899A

Title:

DEVICE AND METHOD FOR AIDING DEALING WITH DETECTION OF COMPUTER VIRUS AND ITS PROCESSING PROGRAM ;

Abstracted Patent: JP2003015899 ;

Publication Date: 2003-01-17 ;

Inventor(s): YOSHIZAWA MITSURU ;

Applicant(s): HITACHI INFORMATION SYSTEMS LTD ;

Application Number: JP20010204176 20010705 ;

Priority Number(s): ;

IPC Classification: G06F11/00; G06F9/44; G06F13/00; G06F17/30; G06F17/60 ;

Equivalents: ;

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a device for aiding dealing with detection of a computer virus capable of reducing the processing load of a manager dealing with computer viruses.SOLUTION: The aiding device 100 is provided with a computer virus dealing database 210 storing at least one of the information on methods dealing with the detection of computer viruses, a retrieving part 240 for retrieving the information on a dealing method corresponding to a computer virus notified by a notification mail notifying the detection of the computer virus in receiving the mail from a client PC 120 by a receiving part 230 and a transmission part 260 for transmitting a reply mail to which the information on the dealing method is attached to the client PC 120 when the information is retrieved.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（A）**　(11)特許出願公開番号
特開2003－15899
（P2003－15899A）
(43)公開日　平成15年１月17日(2003.1.17)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
G06F 11/00		G06F 9/44	560B	5B075
9/44	560	13/00	630A	5B076
13/00	630	17/30	110F	
17/30	110		170Z	
	170	17/60	138	

審査請求 有　請求項の数7　OL　（全 6 頁）　最終頁に続く

(21)出願番号　特願2001－204176(P2001－204176)

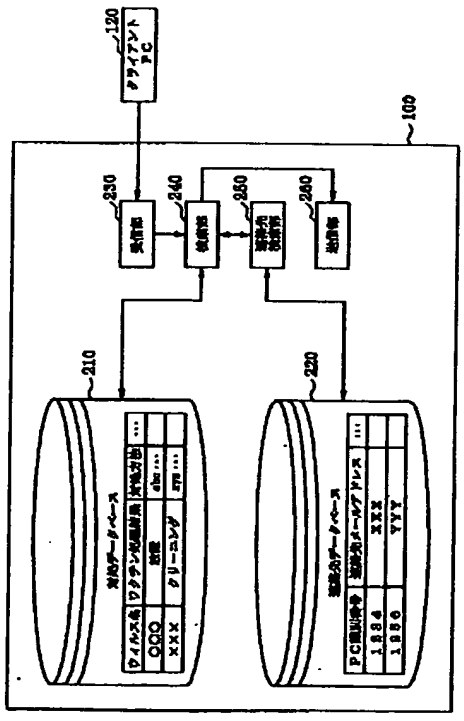
(22)出願日　平成13年７月５日(2001.7.5)

(71)出願人　000152985
株式会社日立情報システムズ
東京都渋谷区道玄坂１丁目16番５号
(72)発明者　吉澤　満
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

Ｆターム(参考)　5B075 KK07 KK13 KK33 KK40 ND20
ND23 PP10 PP14 PP30 PQ05
PQ20 QP10 UU24 UU40
5B076 FD08

(54)【発明の名称】　コンピュータウィルス検出時対処支援装置とその方法およびその処理プログラム

(57)【要約】
【課題】　コンピュータウィルスの対処を行う管理者における処理負担を軽減するコンピュータウィルス検出時の対処支援装置を提供すること。
【解決手段】　本発明に係るコンピュータウィルス検出時対処支援装置１００は、コンピュータウィルスの検出時の対処方法の情報を少なくとも１つ記憶したコンピュータウィルスの対処データベース２１０と、クライアントＰＣ１２０からコンピュータウィルスの検出の通知メールを受信部２３０で受信すると、この通知メールで報告されたコンピュータウィルスに対応する対処方法の情報を、対処データベース２１０から検索する検索部２４０と、対処方法の情報が検索されたならば、この対処方法の情報を添付した返信メールを、クライアントＰＣ１２０に送信する送信部２６０とを有する。



【特許請求の範囲】
【請求項1】　コンピュータウィルスの検出時の対処方法の情報を少なくとも1つ記憶したコンピュータウィルスの対処データベースと、
端末装置からコンピュータウィルスの検出の通知メールを受信すると、該通知メールで報告されたコンピュータウィルスに対応する対処方法の情報を、前記対処データベースから検索する検索手段と、
該対処方法の情報が検索されたならば、該対処方法の情報が添付された返信メールを、前記端末装置に送信する送信手段とを有することを特徴とするコンピュータウィルス検出時対処支援装置。
【請求項2】　コンピュータウィルスの検出時の対処方法の情報を少なくとも1つ記憶したコンピュータウィルスの対処データベースと、
端末装置でコンピュータウィルスの検出の通知メールを受信すると、該通知メールで報告されたコンピュータウィルスに対応する対処方法の情報を、前記対処データベースから検索する検索手段と、
前記端末装置自体に対応して登録された、メールアドレスを記憶する連絡先データベースと、
該対処方法の情報が検索されたならば、該対処方法の情報が添付された返信メールを、前記連絡先データベースに基づいた前記端末装置に対応する前記メールアドレスに送信する送信手段とを有することを特徴とするコンピュータウィルス検出時対処支援装置。
【請求項3】　請求項1または2に記載のコンピュータウィルス検出時対処支援装置において、
前記検索手段で該報告されたコンピュータウィルスの対処方法の情報が検索できなかった場合は、前記送信部は、該通知メールおよび該コンピュータウィルスに対する調査を促す調査依頼メールを、予め登録されたコンピュータウィルス対処を行う管理者宛てのアドレスに送信することを特徴とするコンピュータウィルス検出時対処支援装置。
【請求項4】　端末装置からコンピュータウィルスの検出の通知メールを受信すると、該通知メールで報告されたコンピュータウィルスに対応する対処方法の情報を、コンピュータウィルスの検出時の対処方法の情報を少なくとも1つ記憶した対処データベースから検索し、
該対処方法の情報が検索されたならば、該対処方法の情報が添付された返信メールを、前記端末装置に送信することを特徴とするコンピュータウィルス検出時対処支援方法。
【請求項5】　端末装置でコンピュータウィルスの検出の通知メールを受信すると、該通知メールで報告されたコンピュータウィルスに対応する対処方法の情報を、コンピュータウィルスの検出時の対処方法の情報を少なくとも1つ記憶した対処データベースから検索し、
該対処方法の情報が検索されたならば、該対処方法の情報が添付された返信メールを、前記端末装置自体に対応して登録されたメールアドレスに送信することを特徴とするコンピュータウィルス検出時対処支援方法。
【請求項6】　請求項4または5に記載のコンピュータウィルス検出時対処支援方法において、
該報告されたコンピュータウィルスの対処方法の情報が検索できなかった場合は、該通知メールおよび該コンピュータウィルスに対する調査を促す調査依頼メールを、予め登録されたコンピュータウィルス対処を行う管理者宛てのアドレスに送信することを特徴とするコンピュータウィルス検出時対処支援方法。
【請求項7】　請求項4乃至6のいずれかに記載のコンピュータウィルス検出時対処支援方法における各処理を、コンピュータに実行させるためのコンピュータウィルス検出時対処支援処理プログラム。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、コンピュータウィルスの検出時の対処支援に関し、特に、コンピュータウィルスの対処を行う管理者における処理負担を軽減するコンピュータウィルス検出時の対処支援装置とその方法およびその処理プログラムに関する。
【0002】
【従来の技術】現在、特に企業等の組織内におけるコンピュータウィルス対処方法として、コンピュータウィルス対処ソフトを保護対象の端末装置で常時または定期的に稼動させ、コンピュータウィルスの検出時には、システム管理者に対してその検出情報を電子メールで通知する技術が用いられている。この技術は、例えば、「日経インターネットテクノロジー、1998年5月号」のアンチウィルスソフト（以下、文献1という）の記載にある、コンピュータウィルスが検出された場合、その情報は、端末装置からサーバーを介して、コンピュータウィルスの対処を行う管理者端末装置に即座に伝えられる技術として紹介されている。
【0003】
【発明が解決しようとする課題】しかしながら、上述の文献1に紹介されているコンピュータウィルス対処方法では、以下に示すような実務上の課題・不具合がある。
（1）コンピュータウィルスの検出の通知メールを受信したシステム管理者は、コンピュータウィルス対処ソフトがコンピュータウィルス駆除に成功した等の、特に対処が不要な通知メールについても適宜確認する必要があった。
（2）過去に同一のコンピュータウィルスに対処したことがある場合、システム管理者はその事例を調査してから対処を指示することになり、過去の事例を活かして対処する際でも、その作業に時間がかかっていた。
（3）もしシステム管理者が不在の場合、過去に対処事例がある場合でも、即座に対処できなかった。

（4）システム管理者は、コンピュータウィルスが検出された端末装置自体の他の装置（例えば、コンピュータウィルスの対処を実際に行う部署毎の担当者）に対して対処方法を送信する必要がある時は、その装置のアドレスを調べて対処メールを送信する煩わしさがあった。

【0004】本発明は、上述のような課題に鑑みてなされ、その目的は、コンピュータウィルスの対処を行う管理者における処理負担を軽減するコンピュータウィルスの検出時の対処支援装置とその方法およびその処理プログラムを提供することにある。

【0005】

【課題を解決するための手段】（1）上記目的を達成するために、本発明に係るコンピュータウィルスの検出時の対処支援装置は、コンピュータウィルスの検出時の対処方法の情報を少なくとも1つ記憶したコンピュータウィルスの対処データベースと、端末装置からコンピュータウィルスの検出の通知メールを受信すると、通知メールで報告されたコンピュータウィルスに対応する対処方法の情報を、対処データベースから検索する検索手段と、対処方法の情報が検索されたならば、この対処方法の情報が添付された返信メールを、端末装置に送信する送信手段とを有することを特徴とする。

【0006】（2）また、本発明に係るコンピュータウィルスの検出時の対処支援装置は、コンピュータウィルスの検出時の対処方法の情報を少なくとも1つ記憶したコンピュータウィルスの対処データベースと、端末装置でコンピュータウィルスの検出の通知メールを受信すると、通知メールで報告されたコンピュータウィルスに対応する対処方法の情報を、対処データベースから検索する検索手段と、端末装置自体に対応して登録された、メールアドレスを記憶する連絡先データベースと、対処方法の情報が検索されたならば、この対処方法の情報が添付された返信メールを、連絡先データベースに基づいた端末装置に対応する前記メールアドレスに送信する送信手段とを有することを特徴とする。

【0007】（3）また、上記（1）または（2）におけるコンピュータウィルスの検出時の対処支援装置において、報告されたコンピュータウィルスの対処方法の情報が検索できなかった場合は、送信部は、通知メールおよびコンピュータウィルスに対する調査を促す調査依頼メールを、予め登録されたコンピュータウィルス対処を行う管理者宛てのアドレスに送信することを特徴とする。

【0008】

【発明の実施の形態】以下に本発明の実施の形態を、図1～図3を用いて詳細に説明する。図1は、本発明に係るコンピュータウィルス検出時対処支援装置を含むシステム構成図を示すブロック図である。図2は、図1に示すコンピュータウィルス検出時対処支援装置の構成を説明するためのブロック図である。図3は、図1，2に示すコンピュータウィルス検出時対処支援装置の動作を説明するためのフローチャートである。

【0009】図1を用いて、本発明に係るコンピュータウィルス検出時対処支援装置100が用いられるネットワークシステム1の概略構成を説明する。コンピュータウィルス検出時対処支援装置100、管理者用PC110（PCはパーソナルコンピュータの略）、およびクライアントPC120の各々は、LAN回線（WAN回線であってもよい）130を介して、相互に接続されている。

【0010】管理者用PC110は、コンピュータウィルス対処の指示、コンピュータウィルス検出時対処支援装置100の管理、および、一般のシステム管理業務等に用いられる端末装置である。クライアントPC120は、一般業務等に用いられる、クライアント側の端末装置である。

【0011】ここで、このクライアントPC120では、上述の従来技術で説明したように、コンピュータウィルス対処ソフトが常時または定期的に稼動され、コンピュータウィルスの検出時には、システム管理者（管理者用PC110）に対してその検出情報を電子メールで通知する機能を有している。

【0012】次に、図2を用いて、本発明に係る、図1のコンピュータウィルス検出時対処支援装置100の構成を説明する。コンピュータウィルス検出時対処支援装置100は、対処DB210（DBはデータベースの略）、連絡先DB220、受信部230、検索部240、連絡先検索部250、および送信部260を有して構成されている。

【0013】対処DB210は、各種コンピュータウィルスに対する対処方法に関する情報が記憶されている。この対処DB210は、各コンピュータウィルスに対して、「ウィルス名」、「ワクチン処理結果」、「（具体的）対処方法」などを項目とする少なくとも1つのレコードが記憶されている。なお、この対処方法の情報は、例えば、各種コンピュータウィルス対処ソフトの処理結果、すなわちワクチン処理結果に対して、クライアントPC120を含むネットワークシステム1全体において過去に対処したコンピュータウィルス駆除方法が記載されている。この対処方法の情報は、適宜、コンピュータウィルス検出時対処支援装置100、または管理者用PC110から入力され、対処DB210に記憶される。

【0014】連絡先DB210は、コンピュータウィルス検出の通知メールに付されたクライアントPC120の固有の識別番号（以下、PC識別番号という）に対応した、連絡先となるべくメールアドレスが記憶されている。なお、このPC識別番号は、クライアントPC120の通知に基づいて、図1において図示しないサーバーにより生成される。つまり、クライアントPCにおけるコンピュータウィルス検出の通知は、この図示しないサ

ーバーを介して、コンピュータウィルス検出時対処支援装置１００に通知されることになるが、ここでは便宜的に、クライアントＰＣ１２０自体が通知メールを送信することとして説明していく。また、この連絡先とは、例えば、通知メールに付されたクライアントＰＣ１２０の利用者に代理して、コンピュータウィルスの対処を実際に行う担当者のメールアドレスである。なお、このＰＣ識別番号と、記憶されるメールアドレスとは、一対一の対応情報とは限らず、一対複数の対応関係でもよい。

【００１５】受信部２３０は、ＬＡＮ回線１３０を介して、電子メールを受信する機能を有する。検索部２４０は、クライアントＰＣ１２０の通知メールで報告されたコンピュータウィルスに対応する対処方法の情報を、対処ＤＢ２１０を参照して検索する。また、検索部２４０は、所望の検索結果が検出された場合、この検出結果、つまりコンピュータウィルスの対処方法の情報を、通知メールに対する返信メールに添付する。なおここで、この返信メールとは、通知メールを送信したクライアントＰＣ自体に対するメールとは必ずしも限らず、他のクライアントＰＣを利用する代理受信者に対してのメールも意味している。つまり、送信元に対する返信、という意味では限定していない。

【００１６】連絡先検索部２５０は、連絡先ＤＢ２２０を参照して、通知メールを送信したクライアントＰＣ自体ではなく、代理受信を行う者のメールアドレスを検索する。送信部２６０は、返信メールを送信する。

【００１７】次に、図３のフローチャートを用いて、コンピュータウィルス検出時対処支援装置１００の動作を説明する。クライアントＰＣ１２０で、コンピュータウィルスが検出されると、この検出に対する通知メールが作成され、自動的に、コンピュータウィルス検出時対処支援装置１００に送信される。

【００１８】受信部２３０は、この通知メールを受信する（ステップＳ３０１）。検索部２４０は、通知メールの本文より、コンピュータウィルス名、そのワクチン処理結果、ＰＣ識別情報などの情報を取り出す（ステップＳ３０２）。検索部２４０は、このワクチン処理結果に基づいて、そのコンピュータウィルスへの対処が必要か否かの判断を行う（ステップＳ３０３）。対処が不要と判断されたならば、以降の処理を終了する。対処が必要と判断されたならば、取得したコンピュータウィルス名およびワクチン処理結果に基づいて、対処ＤＢ２１０を参照して、これと一致する対処方法を検索する（ステップＳ３０４）。一致する対処方法が検出されれば、検索部２４０は、この対処方法の情報を取り出す。一致する対象方法が検出されなければ、以降の処理を終了、あるいは、後述するステップＳ３０７の処理を行う。

【００１９】上記ステップＳ３０４で一致する対処方法が検出されると、連絡先検索部２５０は、連絡先ＤＢ２２０を参照して、通知メールの発信元のクライアントＰＣのＰＣ識別番号を基に、これと対応する連絡先メールアドレスを検索する。（ステップＳ３０５）。例えば、図２の連絡先ＤＢ２２０のＰＣ識別番号「１２３４」に対応する、連絡先メールアドレス「ＸＸＸ」が検出されることになる。送信部２６０は、検索されたメールアドレスに対して、対処方法の情報が添付された返信メールを送信する（ステップＳ３０６）。

【００２０】なお、上記ステップＳ３０４で一致する対処方法が検出されなかった場合、送信部２６０が、システム管理者に、通知メールを転送すると共に、このコンピュータウィルスに対する調査を促す調査依頼メールを送信するようにしてもよい（ステップＳ３０７）。

【００２１】このように、本発明に係るコンピュータウィルスの検出時対処支援装置を用いることで、コンピュータウィルスの対処を行う管理者における処理負担を軽減することができる。

【００２２】なお、本発明は、上述の図１～図３を用いて説明した例に限定されるものではなく、その要旨を逸脱しない範囲において種々の変更が可能である。例えば、上記ステップＳ３０５においては、コンピュータウィルスが検出されたクライアントＰＣからの通知メールのＰＣ識別情報を参照しているが、この通知メールがクライアントＰＣから送信される際に、そのＰＣを利用管理する者のメールアドレスがその通知メールに付されるようにしておき、この利用管理者のメールアドレスに対して返信するようにしてもよい。この場合、図２の連絡先ＤＢ２２０の「ＰＣ識別番号」は、「利用管理者のメールアドレス」として登録することになる。

【００２３】またこれに関連して、上述の実施形態のステップＳ３０５において、特に、図２における連絡先ＤＢ２２０から検出されたメールアドレスを用いて返信メールを送信していたが、この連絡先ＤＢ２２０を用いないで、上記利用管理者でなく、直接に、通知メールの送信元のクライアントＰＣに、返信メールを送信するようにしても当然によい。

【００２４】また、上述の実施形態では、図１におけるコンピュータウィルスの検出時対処支援装置１００に、対処ＤＢ２１０および連絡先ＤＢ２２０を設けていたが、この対処ＤＢ２１０および連絡先ＤＢ２２０を、ＬＡＮ回線１３０上のいずれかに移行させて運用してもよい。この場合、コンピュータウィルスの検出時対処支援装置は、この対処ＤＢ２１０および連絡先ＤＢ２２０が格納された新たな装置と、データの送受信を行うための処理部を介して行われることになる。なお、ＬＡＮ回線１３０ではなく、ＷＡＮ回線を介して構築したコンピュータウィルスの検出時対処支援のシステムにおいても、同様の効果を奏することができる。

【００２５】また、上述の実施形態のステップＳ３０７の処理ではなく、通知メールの内容を含み、このコンピュータウィルスに対する調査を促す1通のメールからな

る調査依頼メールを送信するようにしてもよい。

【0026】また、上述の実施形態のステップS303において、特に、クリーニングであれば対処はなく通知不要との意味から、ワクチン処理結果の判断処理を行っていた。しかし、この対処が不要との返信メールを送信するものとすれば、このステップS303における処理を省略して、実行することとしてもよい。

【0027】上述の実施形態および上記種々の変更形態において、その処理を行うプログラムをアプリケーションソフトとして、ハードディスク等の記録媒体に格納しておいてもよい。このようにすれば、CD-ROM等の可搬型記録媒体にプログラム等を格納して売買したり、携帯することができるようになる。

【0028】

【発明の効果】本発明に係るコンピュータウィルス検出時対処支援装置を用いることで、以下に挙げられるような効果を得ることができる。

(1) コンピュータウィルスの検出の通知メールを受信したシステム管理者は、特に対処が不要な通知メールについて適宜確認する必要がなくなる。

(2) 過去の対処事例を活かして、即座に対処することができる。

(3) もしシステム管理者が不在の場合、過去に対処事例がある場合でも、即座に対処できる。

(4) システム管理者は、コンピュータウィルスが検出された端末装置自体の他の装置（例えば、コンピュータウィルスの対処を実際に行う部署毎の担当者）に対してメールアドレスを調べてから、対処方法を送信するという煩わしさがなくなる。このように、本発明に係るコンピュータウィルス検出時対処支援装置により、コンピュータウィルスの対処を行う管理者における処理負担を軽減することができる。

【図面の簡単な説明】

【図1】本発明に係るコンピュータウィルス検出時対処支援装置を含むシステム構成図を示すブロック図である。

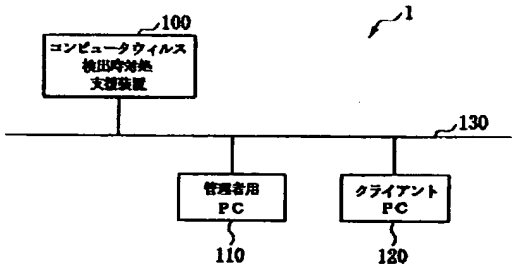
【図2】図1に示すコンピュータウィルス検出時対処支援装置の構成を説明するためのブロック図である。

【図3】図1，2に示すコンピュータウィルス検出時対処支援装置の動作を説明するためのフローチャートである。

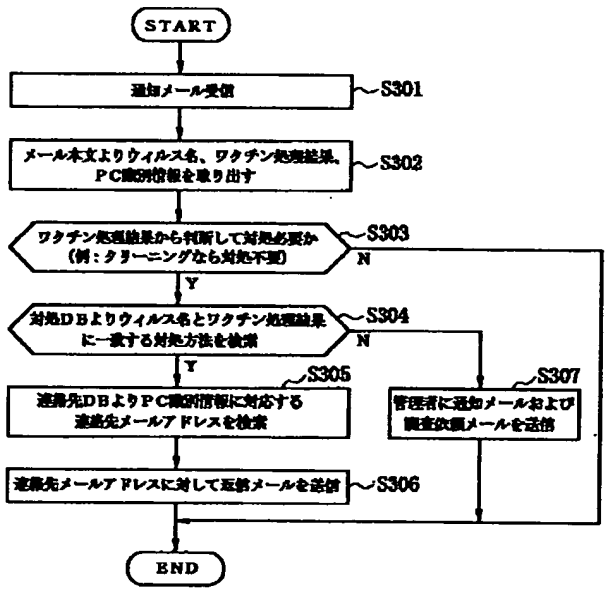
【符号の説明】

100：コンピュータウィルス検出時対処支援装置
110：管理者用PC
120：クライアントPC
130：LAN回線
210：対処データベース
220：連絡先データベース
230：受信部
240：検索部
250：連絡先検索部
260：送信部

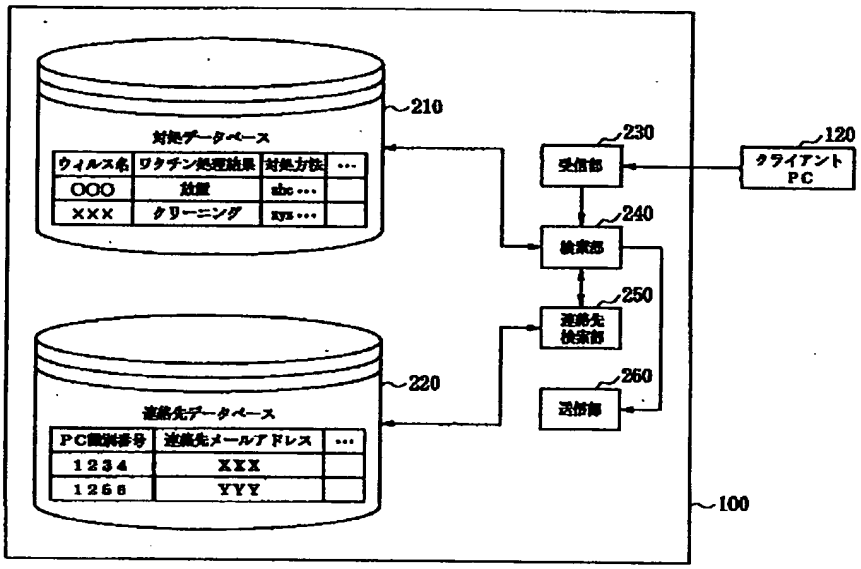
【図1】



【図3】



【図2】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
G06F 17/60	138	G06F 17/60	174	
	174		9/06	660N